# Statement of SCAP implementation

The Security Content Automation Protocol (SCAP) is a collection of six open standards developed jointly by various United States government organizations and the private sector. Security content conforming to the SCAP standard can be used by any product that supports the standard and the results can be shared among these products.

McAfee Policy Auditor 5.2 provides the ability to detect and assess a single system or thousands of systems from a Policy Auditor Server. This standardization allows regulatory authorities and security administrators to construct definitive security guidance and to compare results reliably and repeatedly.

Policy Auditor is an enterprise product designed exclusively around SCAP and manages all aspects of analyzing systems for compliance. The product provides an implementation for SCAP standards. It uses the eXtensible Configuration Checklist Description Format (XCCDF) and Open Vulnerability and Assessment Language (OVAL) assessment protocols to determine which items to check on a system and how to check them.

Policy Auditor allows users to import and export benchmarks and checks that use SCAP. Users can tailor or edit benchmarks within the McAfee Benchmark Editor interface and activate them for use in audits. Benchmarks determine whether a system complies with the benchmark rules. Benchmarks also return results that can be converted to a human-readable format.

Benchmarks and checks incorporate the following reference protocols to ensure that all rules are processed accurately and appropriately, and that the results appear properly in reports and export files:

- Common Vulnerabilities and Exposures (CVE)
- Common Configuration Enumeration (CCE)
- Common Platform Enumeration (CPE)
- Common Vulnerability Scoring System (CVSS)

# Statement of CVE implementation

McAfee Policy Auditor 5.2 fully implements and supports the Common Vulnerabilities and Exposures (CVE) standard vulnerability dictionary. CVE provides unique, standardized identifiers for security vulnerabilities. CVE does not address compliance items, only vulnerability issues.

Each CVE identifier consists of:

- A CVE identifier number, such as CVE-2008-0042.
- An indication of whether the CVE has a status of "entry" or "candidate."
- A description of the vulnerability.
- A list of any references, such as advisories or OVAL identification.

Policy Auditor implements and supports the CVE enumeration, which provides standardized references to known vulnerabilities. CVE uses a named list of information security weaknesses, providing standardized identifiers to facilitate a universal naming convention.

Policy Auditor patch and vulnerability definitions are updated periodically when new content is available. The audit results can be viewed from the Audits, Reports, or Dashboard user interfaces.

CVE information is accessible from the Checks interface, which displays details of Common Vulnerabilities. Users have the ability to view even more detailed CVE information from the Check Details page, which displays the Source, ID, and URL. For example, the URL http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-2122 refers the user to the Mitre site to view details about CVE-2005-2122. The security content provided by McAfee refers to CVE identifiers when addressing vulnerabilities and whether a vendor's patch has been applied to address the vulnerability.

Previous versions of Policy Auditor have been certified by Mitre as CVE-Compatible.

# Statement of CCE implementation

McAfee Policy Auditor 5.2 incorporates and supports version 5.0 of the Common Configuration Enumeration (CCE) standard.
CCE provides a standard system for identifying and referencing system configuration settings. It identifies the configuration itself, not the means by which that configuration was reached. CCE encourages interoperability, improves the correlation of test results, and simplifies gathering metrics.
Policy Auditor includes CCE references in the checks content. The Checks tab lists all the checks available to users. Clicking on a check with CCE content lists CCE references that identify the CCE system configuration settings.
Previous versions of Policy Auditor have been certified by Mitre as CCE-Compatible.

# Statement of CPE implementation

McAfee Policy Auditor 5.2implements version 2.1 of the Common Platform Enumeration (CPE) standard. CPE provides a standard reference and notation method for information technology systems, platforms, and packages.
Policy Auditor contains the CPE data dictionary in the database with some of it in aggregated format to promote ease of use. Information from this dictionary drives various aspects of the Policy Auditor interface. Policy Auditor associates OVAL definitions with CPE Names and allows users to specify CPE names at the benchmark, group, profile, or rule level. Policy Auditor allows users to create audits with SCAP content that covers a number of common operating systems and platforms.
When CPE platforms are specified, Policy Auditor uses this information to determine whether it should evaluate compliance with a rule or group of rules. For example, an audit can cover both Windows XP and Windows Vista operating systems but not the Windows 2000 operating system. CPE allows Policy Auditor to use the correct content on the correct systems.
Previous versions of Policy Auditor have been certified by Mitre as CPE-Compatible.

# Statement of CVSS implementation

McAfee Policy Auditor 5.2 incorporates version 2.0 of the Common Vulnerability Scoring System (CVSS). CVSS is a standardized open framework for measuring the impact of vulnerabilities. Each CVE includes an associated CVSS vector to determine the relative severity of vulnerabilities. CVSS is built on a quantitative model that ensures repeatable measurements on systems, valid comparisons between systems, and that allows users to view the underlying vulnerability characteristics. Using CVSS scores can help an organization determine and prioritize responses to detected vulnerabilities.
Policy Auditor supports all four standard SCAP scoring models:

- Flat
- Unweighted
- Absolute
- Default

The default setting for Policy Auditor is a flat unweighted scoring model normalized to a maximum

possible score of 100. The scoring model can be changed for comparison purposes.
Previous versions of Policy Auditor have been certified by Mitre as CVSS-Compatible.

# Statement of XCCDF implementation

McAfee Policy Auditor 5.2 provides an implementation of version 1.1.4 of the eXtensible Configuration Checklist Description Format (XCCDF). XCCDF supports the exchange of information, results document generation, tailoring, automated compliance testing, and compliance scoring. It also provides a data model and format for storing results of benchmark compliance testing. The goal of XCCDF is to provide a uniform standard for the expression of benchmarks and other configuration guidance to encourage good security practices.
Policy Auditor uses benchmarks from McAfee or third-party sources to construct audits. Users can select the benchmark profile, if any, to use for the audit. After a system is audited, the audit results are returned to Policy Auditor, which analyzes and reports on the configuration and vulnerability data. The user can specify how long audit data is retained so that they or auditors can review any changes in the state of a system over time.
Previous versions of Policy Auditor have been certified by Mitre as XCCDF-Compatible.

# Statement of OVAL implementation

Policy Auditor 5.2implements and supports version 5.5 of the Open Vulnerability and Assessment Language (OVAL). OVAL is an international standard that promotes openly-available security content. It is the common language for security experts to check for the presence of vulnerabilities and configuration issues on computer systems. OVAL provides a structured model for network and system administrators to detect vulnerabilities and configuration issues on systems.
Policy Auditor uses the Checks interface to import and export OVAL definitions and other formats supported by XCCDF. These checks can be filtered based on OVAL IDs, platforms, or any other criteria set by the user. The Check Details interface displays a hyperlink to specific OVAL IDs, which will display OVAL in XML format.
When a system is audited, the OVAL content is processed according to the information in the XCCDF benchmarks contained in the audit. The OVAL content captures the state of the system at the particular point in time that the audit is run. The results are returned to Policy Auditor for analysis and reporting. The user specifies how long audit data is to be retained so that they or auditors can review any changes in the state of a system over time.
Previous versions of Policy Auditor have been certified by Mitre as OVAL-Compatible.